

# Configuring AppleTalk Remote Access

---

This chapter describes how to configure your router to act as an AppleTalk Remote Access (ARA) server. It does not describe how to configure or use the client Macintosh. Refer to the Apple Computer, Inc. *Apple Remote Access Client User's Guide* and the *Apple Remote Access Personal Server User's Guide* for information about how to set up and use the ARA software on your Macintosh.

For a complete description of the commands in this chapter, refer to the "AppleTalk Remote Access Commands" chapter of the *Dial Solutions Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

## AppleTalk Remote Access

The Cisco implementation of ARA gives Macintosh users direct access to information and resources in remote AppleTalk networks over standard telephone lines. For example, if you have a PowerBook at home and need to get a file from your Macintosh at the office, ARA software can make the connection between your home and office computers over telephone lines.

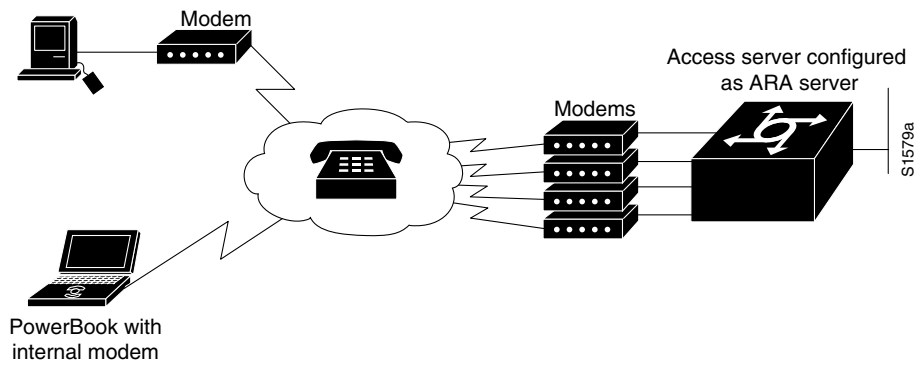
You can configure your router to act as an ARA server by enabling AppleTalk and ARA protocol on physical terminal (TTY) or virtual terminal (VTY) lines. Configuring your router to act as an ARA server allows remote Macintosh users to dial in, become a network node, and connect to devices on other networks. ARA protocol support is transparent to the Macintosh end user. Macintosh users can also use Serial Line Internet Protocol (SLIP) to access remote IP network resources and Point-to-Point Protocol (PPP) to access both AppleTalk and IP resources.

The following Macintosh and Cisco IOS software support is required for ARA connectivity:

- Macintosh running ARA software and a connection control language (CCL) script.
- Router configured as an ARA server.

Figure 98 shows how your router can act as an ARA server between remote Macintosh computers (in Figure 98, a Power Macintosh and a PowerBook) and devices on another network.

**Figure 98 ARA Configuration Overview**



## ARA Configuration Task List

To set up the Cisco IOS software to act as an ARA server, complete the following tasks:

- Connect Cables
- Configure the Line and the Modem
- Configure ARA Required Tasks

The following tasks are optional:

- Configuring ARA Optional Tasks
- Configure ARA Security
- Connect to an AppleTalk Network from a Client Running a Different Virtual Terminal Protocol

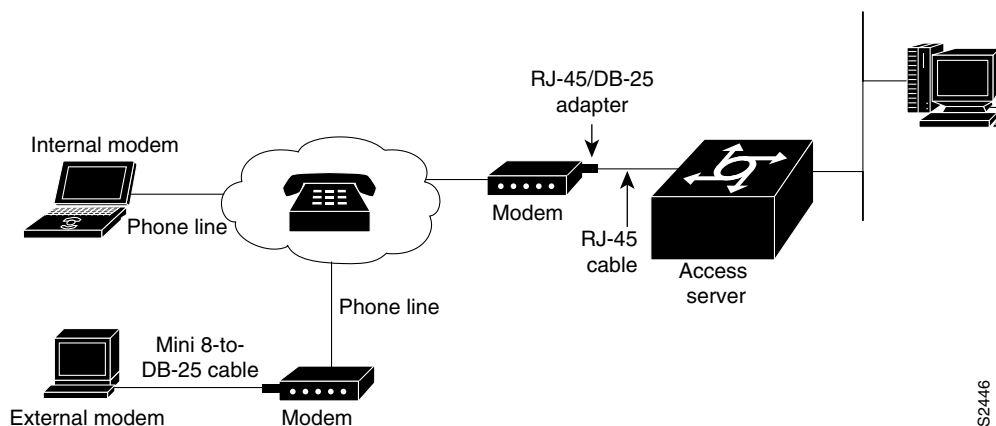
To enable asynchronous callback to ARA clients, refer to the section “Call Back ARA Clients” in the “Configuring Asynchronous Callback” chapter.

To enable remote clients running PPP to dial in and access AppleTalk resources on a network, you must configure AppleTalk over PPP (referred to as ATCP). To configure ATCP, refer to the section “Configure AppleTalk-PPP” in the chapter “Configuring Asynchronous PPP and SLIP.”

## Connect Cables

Figure 99 shows how to connect a Macintosh using internal and external modems.

**Figure 99 ARA Server Cabling and Connections**



Use the MMOD version of the RJ-45-to-DB-25 adapter (labeled “Modem” if the adapter is from Cisco) to connect a “rolled” RJ-45 cable from the router to the modem. Use a high-speed modem cable with hardware flow control to connect a modem to your Macintosh (refer to the user documentation for your modem for more specific information).

For more information about connecting cables, refer to the installation and configuration or product user guide that came with your router.

## Configure the Line and the Modem

Configure the line as follows:

**Step 1** Specify the maximum common line speed for the modem and the access server. The access server supports 4x compression of data, so you can typically use the speeds shown in the following list:

- 115200 bps for use with modems that support a transmission rate of 28800
- 57600 bps for use with modems that support a transmission rate of 14400
- 38400 bps for use with modems that support a transmission rate of 9600

---

**Note** Refer to your modem guide to ensure that the modem can support these maximum line speeds.

---

**Step 2** Set hardware flow control—Use the **flowcontrol hardware** command to enable hardware flow control.

---

**Note** The Cisco IOS software does not support modems that do not support hardware flow control.

---

**Step 3** Specify your modem control parameters—Use the **modem inout** command to configure the line for both incoming and outgoing calls, or use the **modem dialin** command to configure the line for incoming calls only.

**Step 4** Configure security on your dialin lines—Use the **aaa new-model** command to enable the authentication, authorization, and accounting (AAA) process on the router, the **aaa authentication arap** command to create an authentication list, and **arap authentication** command to apply the authentication list to a line or set of lines configured for ARA.

For more information about configuring lines and modem control, refer to the chapter “Configuring Modem Support and Asynchronous Devices” in this publication. For information about configuring security, refer to the *Security Configuration Guide*.

---

**Note** The **autobaud** command is not supported with ARA and should never be used.

---

## Configure ARA Required Tasks

To allow ARA connections to pass through the access server or router, perform the following tasks beginning in global configuration mode:

Step	Command	Purpose
1	<b>appletalk routing</b>	Enable AppleTalk. <sup>1</sup>
2	<b>arap network</b> <i>[network-number]</i> <i>[zone-name]</i>	Create a new network or zone for ARA clients when they dial in. The <i>network-number</i> argument must be a unique network number.
3	<b>appletalk send-rtmps</b>	In interface configuration mode, ensure that a new internal network is advertised by enabling the Routing Table Maintenance Protocol (RTMP).
4		Configure an AppleTalk interface using the discovery mode in the Cisco IOS software. To do so, an interface on the router must be connected to a network that has at least one other router configured for AppleTalk.
5	<b>appletalk routing</b>	Return to global configuration mode and turn on AppleTalk routing.
6	<b>line</b> <i>[tty   aux   vty]</i> <i>line-number</i> <i>[ending-line-number]</i>	Enter line configuration mode.
7	<b>arap enable</b>	Enable ARA on a line.

1. For more information about configuring AppleTalk, refer to the chapter “Configuring AppleTalk” in the *Network Protocols Configuration Guide, Part 2*.

If you discover that the AppleTalk network already exists when you get to Step 4, the zone and cable range must match the existing configuration. To identify existing cable ranges and zone names, configure the Cisco IOS software for discovery mode. You must manually configure an AppleTalk interface on a segment for which there are no AppleTalk routers. For more information, refer to the chapter “Configuring AppleTalk” in the *Network Protocols Configuration Guide, Part 2*.

## Configuring ARA Optional Tasks

Refer to this section after you have configured AppleTalk routing, created an internal ARA network or zone, and enabled ARA. At this point, you can enable optional tasks. Though optional, the tasks in this section *might* be required for your network environment.

To configure the Cisco IOS software to allow an ARA session to start automatically, perform the following tasks beginning in global configuration mode:

Step	Command	Purpose
1	<b>autoselect</b> { <b>arap</b>   <b>ppp</b>   <b>slip</b>   <b>during-login</b> }	Configure a line to automatically start an ARA session.
2	<b>line x</b> (x = the line you want to configure in Step 3)	Enter line configuration mode.
3	<b>arap dedicated</b>	Enter line configuration mode and dedicate a line to function only as an ARA connection.
4	<b>arap timelimit</b> [ <i>minutes</i> ]	Set the maximum length of an ARA session for a line. The default is to have unlimited length connections.
5	<b>arap warningtime</b> [ <i>minutes</i> ]	Set when a disconnect warning message is displayed, in number of minutes before the line is disconnected. This command is valid only when a session time limit is set.

The **autoselect** command permits the router to start an ARA session automatically when it detects the start character for an ARAP packet. The Cisco IOS software detects either a Return character, which is the start character for an EXEC session, or the start character for the ARA protocol. By issuing the **autoselect** command with the **during-login** argument, you can display the username or password prompt without pressing the Return key. While the username or password prompts are displayed, you can choose to answer these prompts or to start sending packets from an autoselected protocol.

Normally a router avoids line and modem noise by clearing the initial data received within the first one or two seconds. However, when the autoselect PPP feature is configured, the router flushes characters initially received and then waits for more traffic. This flush causes time out problems with applications that send only one carriage return. To ensure that the input data sent by a modem or other asynchronous device is not lost after line activation, enter the **flush-at-activation** line configuration command.

For information about using ARA with TACACS, Extended TACACS, and AAA/TACACS+, refer to the section “Configure ARA Security” in this chapter and the *Security Configuration Guide*.

---

**Note** When you use the autoselect function, the activation character should be set to the default, Return, and exec-character-bits to 7. If you change these defaults, the application cannot recognize the activation request.

---

To customize the AppleTalk configuration even further, you can perform the following additional tasks:

- Disable Checksum Generation and Verification
- Configure MacIP

For more information about these and other tasks you can perform to customize your AppleTalk configuration, refer to the chapter “Configuring AppleTalk” in the *Network Protocols Configuration Guide, Part 2*.

## Configure ARA Security

The following three types of security can be used with ARA:

- ARA Server Security, including required manual password entry, limited network visibility, and no guest access.
- Local or Remote Security Database, including username and password authentication and access lists.
- TACACS and TACACS+ Security for ARA, including TACACS, TACACS+/AAA, and Kerberos.

The following sections describe these tasks. Refer to the *Security Command Reference* for information about commands listed in these tasks.

### ARA Server Security

This section describes the following security features that are specific to the ARA protocol:

- Require Manual Password Entry
- Limit Network Visibility
- Disallow Guests

#### Require Manual Password Entry

You can control access by requiring users to enter their password manually at the time they log in. To force manual password entry, perform the following task in line configuration mode:

Command	Purpose
<b>arap require-manual-password</b>	Require manual password entry.

#### Limit Network Visibility

You can control Macintosh access to zones and networks by using **arap** commands to reference access control lists configured using AppleTalk **access-list** commands.

To control which zones the Macintosh user can see, perform the following task in line configuration mode:

Command	Purpose
<b>arap zonelist</b> <i>zone-access-list-number</i>	Limit the zones the Macintosh user sees.

To control traffic from the Macintosh to networks, perform the following task in line configuration mode:

Command	Purpose
<b>arap net-access-list</b> <i>net-access-list-number</i>	Control access to networks.

## Disallow Guests

A guest is a person who connects to the network without having to give a name or a password. To prohibit Macintosh guests from logging in through the router, perform the following task in line configuration mode. Use the optional **if-needed** argument to allow users to log in as guests if they are already authenticated with a username or password.

Command	Purpose
<b>arap nologuest</b> [if-needed]	Prohibit guests from logging in to the ARA network.



**Caution** Do not use the **arap nologuest** command if you are using modified CCL scripts and the **login tacacs** command.

## Local or Remote Security Database

To prevent unauthenticated users from accessing your network resources, you configure a username and password database. This database can be local on the router or can be stored on a remote security server (a PC or UNIX computer set up with a security database). Perform the tasks in the following sections to configure the Cisco IOS software to support either local or remote authentication:

- Configure Local Username Authentication
- Enable Remote TACACS or TACACS+ Server Authentication

### Configure Local Username Authentication

To configure internal username authentication, perform the following task in global configuration mode. Enter this information for each supported user.

Command	Purpose
<b>username</b> <i>name</i> <b>password</b> <i>password</i>	Specify a username and password.

When users try to log in to the access server, username and password prompts require them to authenticate themselves before they can have access to the router or the network.

### Enable Remote TACACS or TACACS+ Server Authentication

To enable the Cisco IOS software to use a remote TACACS or TACACS+ authentication database, perform the following tasks in global configuration mode:

Step	Command	Purpose
1	<b>tacacs-server host</b> { <i>hostname</i>   <i>ip-address</i> }	Specify the IP address or the host name of the remote TACACS+ server host. This host is typically a UNIX system running TACACS+ software.
2	<b>tacacs-server key</b> <i>shared-secret-text-string</i>	Specify a shared secret text string used between the router and the TACACS+ server. The router and TACACS+ server use this text string to encrypt passwords and exchange responses.

After you specify these commands in the Cisco IOS software, you must populate the remote username database to all users to whom you want to provide network access. When users try to log in to the router, username and password prompts require them to authenticate themselves before they can have access to the router or the network.

## TACACS and TACACS+ Security for ARA

You can prevent unauthenticated users from accessing your network resources using the following security mechanisms:

- TACACS and AAA/TACACS+ user authentication, with username and password information stored on a TACACS or TACACS+ server
- Kerberos, which is configured through the AAA facility

For more information about each of these security mechanisms, refer to the *Security Configuration Guide*.

Perform the tasks in the following sections to configure TACACS and TACACS+ security to authenticate clients that are using ARA to dial in:

- Enable Standard and Extended TACACS for ARA Authentication
- Enable AAA/TACACS+ for ARA Authentication
- Modify Scripts to Support a Standard EXEC Security Dialog—This is only necessary if you are running Standard TACACS on both your router and your TACACS server.

### Enable Standard and Extended TACACS for ARA Authentication

To use Extended TACACS, you must already have set up an Extended TACACS server using the Cisco Extended TACACS server software, available from the [ftp.cisco.com](http://ftp.cisco.com) directory. Refer to the README in this directory for more information. There are two authentication methods used with standard TACACS:

- You issue the **arap use-tacacs** command. The remote user logs in by entering the appropriate username at the ARA username prompt and password at the password prompt.
- You issue the **arap use-tacacs** command and the **single-line** keyword. The remote user logs in by entering *username\*password* at the ARA username prompt, and **arap** at the password prompt.

---

**Note** The **arap use-tacacs** command provides TACACS security without having to modify CCL scripts and respond to dialog boxes. The use of scripts is still a supported feature, and is described in the section “Modify Scripts to Support a Standard EXEC Security Dialog” later in this chapter.

---

To configure the router to authenticate using TACACS, perform one of the following task in line configuration mode:

Step	Command	Purpose
1	<b>arap use-tacacs</b> [ <b>single-line</b> ]	Enable TACACS under ARA.
2	<b>login tacacs</b>	Enable login authentication using TACACS.

For an example of enabling TACACS for ARA authentication, see the section “ARA Configuration Examples” later in this chapter.

## Enable AAA/TACACS+ for ARA Authentication

To enable TACACS+ authentication for ARA sessions, perform the following tasks, beginning in global configuration mode:

Step	Command	Purpose
1	<b>aaa new-model</b>	Enable the authentication, authorization, and accounting (AAA) function in the Cisco IOS software.
2	<b>aaa authentication arap   login {default   list-name} method1 [...method4]</b>	Create an authentication list that you later apply to lines configured for ARA sessions or log in to the router.
3	<b>line [tty] line-number [ending-line-number]</b>	Enter line configuration mode.
4	<b>arap authentication {default   list-name}</b>	Apply an ARA authentication list to lines configured for ARA.
5	<b>login authentication {default   list-name}</b>	Apply a login authentication list to lines that users can log in to.

### Modify Scripts to Support a Standard EXEC Security Dialog

This section describes how to modify your CCL script to work with TACACS security and how to configure a line to use a TACACS server for user authentication.



**Caution** Because of the underlying structure of the ARA protocol, modem layer error control is disabled during the exchange of username and password. This makes the exchange highly susceptible to line noise, especially at higher baud rates enabled by V.34 modems. For this reason, Cisco does not recommend the use of modified scripts and encourage users to either upgrade to later versions of TACACS or to use the **arap use-tacacs single-line** command.

For information on how to use TACACS without modifying scripts, refer to the “Enable Standard and Extended TACACS for ARA Authentication” section in this chapter. For information about the **arap** commands, refer to the *Dial Solutions Command Reference*.

If you are currently using modified CCL scripts and want to migrate to nonmodified scripts, see the section “Configure Modified and Unmodified Scripts Example” at the end of this chapter for information on how to use both in the same environment.

For several popular modems, Cisco provides CCL files that you can use as examples to modify your CCL scripts to support TACACS security. This section explains how to use the CCL files provided by Cisco with TACACS security.

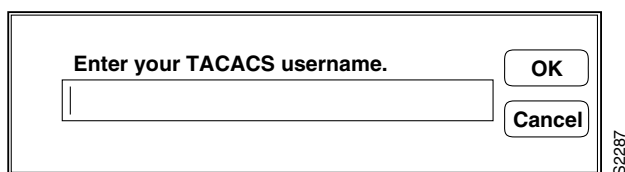
For more information about standard modem initialization scripts, refer to the appendix “Configuring Modem Support and Chat Scripts” in the *Dial Solutions Command Reference*. Cisco recommends using the ARA Modem Toolkit provided through the AppleTalk Programmers and Developers Association (APDA); it provides both syntax checking and a script tester.

The Macintosh client uses ARA CCL scripts to establish point-to-point links with the modem to the AppleTalk network. When the connection has been established, the script ends and ARA is activated. TACACS authentication occurs after the connection is established and the ARA script ends, but before the ARAP protocol becomes active.

Insert TACACS logic just before the end of a script. The CCL TACACS logic performs the following user authentication tasks:

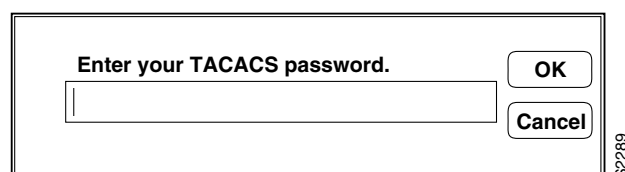
- 1 When the “Username:” prompt is received from the router, the TACACS server queries the user for a username, as shown in Figure 100.

**Figure 100 TACACS Login Screen on the Macintosh Computer**



- 2 When the "Password:" prompt is received from the router, the TACACS server queries the user for a password, as shown in Figure 101.

**Figure 101 TACACS Password Screen on the Macintosh Computer**



- 3 After a successful login, indicated by an EXEC prompt, the **arap** EXEC command is executed.
- 4 The script ends and ARA is activated on the client.

CCL scripts control logical flow by jumping to labels. The labels are the numbers 1 through 128 and are not necessarily in sequential order in script files. The TACACS logic in the Cisco IOS software CCL files has label numbers from 100 through 127. In most environments, you can copy the complete TACACS logic from a sample file.

To create a new TACACS CCL file, perform the following steps:

- Step 1** Copy the TACACS logic from a sample CCL script into the new CCL script.

In most cases, you can insert the TACACS logic at the appropriate place in your CCL script. The one case that requires extra attention is when the original CCL script has labels that conflict with the logic in the new file. The labels must be resolved on a case-by-case basis, usually by changing the label numbers used in the original CCL script. Be sure to read the manual that comes with the Modem Toolkit before beginning.

- Step 2** Locate the logical end of the CCL script and insert the command **jump 100**.

You can locate the logical end of the script by following its flow. Most scripts have the following basic structure:

- Initialize the modem
- Dial the number
- Exit

The characteristic logical end of the script is as follows:

```
@label N
! N is any integer between 1 and 128
if ANSWER N+1
! If we're answering the phone, jump directly
! to the label N+1
```

```

pause 30
! We're not answering the phone, therefore we
! must be calling. Wait three seconds for the
! modems to sync up.
@label N+1
exit 0
! quit and start up ARA

```

It is common in this case to replace “pause 30” with “jump 100.” In fact, this is usually the only change made to the logic of the original CCL script.

Refer to the “Configuring Modem Support and Asynchronous Devices” chapter in this publication for information about configuring a line to support your modem.

### Enable Kerberos Security for ARA Authentication

You can use Kerberos as an authentication method within ARA sessions. To do so, you configure Kerberos using the AAA/TACACS+ facility in the Cisco IOS software. Perform the following tasks in global configuration mode to enable Kerberos security:

Step	Command	Purpose
1	<b>kerberos local realm</b> { <i>kerberos-realm</i> }	Define the name of the Kerberos realm in which the router is located.
2	<b>kerberos realm</b> { <i>dns-domain</i>   <i>dns-host</i> } <i>kerberos-realm</i>	Define the DNS domain of the Kerberos realm in which the router is located.
3	<b>show kerberos creds</b>	Display the contents of your credentials cache.
4	<b>clear kerberos creds</b>	Delete the contents of your credentials cache.

For more information about Kerberos authentication, refer to the *Security Configuration Guide*.

### Use Access Lists to Control Access to AppleTalk Networks

An access list is a list of AppleTalk network numbers or zones that is maintained by the Cisco IOS software and used to control access to or from specific zones or networks. For more information about AppleTalk access lists, refer to the section “Control Access to AppleTalk Networks” in the chapter “Configuring AppleTalk” in the *Network Protocols Configuration Guide, Part 2*.

## Connect to an AppleTalk Network from a Client Running a Different Virtual Terminal Protocol

ARA can run on any point-to-point link, such as a Public Switched Telephone Network (PSTN) or an X.25 WAN. This permits remote Macintosh users to dial in to a remote network and access AppleTalk services (such as file sharing and printing). For example, you can enable a Macintosh client on the remote side of an X.25 WAN to connect to an AppleTalk network through the router. To do so, you configure a virtual terminal (VTY) line on the router so that the client sees one of two scenarios:

- A client clicks **Connect** in an ARA application dialog box and connects to a VTY line on the router. ARA automatically starts up on the outgoing VTY line, and the client is connected to the AppleTalk network. This section describes how to configure the Cisco IOS software for this process.
- A client clicks **Connect** in an ARA application dialog box and connects directly through the router to the AppleTalk network. This process is described in the section “Configure Tunneling of SLIP, PPP, or ARA” in the chapter “Configuring Protocol Translation and Virtual Asynchronous Devices.”

To enable ARA on VTY lines and enable clients running different virtual terminal protocols to connect to an AppleTalk network through the router, perform the following tasks, beginning in global configuration mode. The first four steps are required. The next eight steps ( through ) are optional. , configure automatic protocol startup, dedicates the line to ARA.

Step	Command	Purpose
1	<b>appletalk routing</b>	Turn on AppleTalk routing.
2	<b>arap network</b> <i>[network-number]</i> <i>[zone-name]</i>	Create an internal AppleTalk network.
3	<b>line vty</b> <i>line-number</i> <i>[ending-line-number]</i>	Enter line configuration mode.
4	<b>arap enable</b>	Enable ARA on a line.
5	<b>autocommand arap</b>	Configure automatic protocol startup.
6	<b>arap dedicated</b>	Set a dedicated ARA line.
7	<b>arap timelimit</b> <i>[minutes]</i>	Set the session time limit.
8	<b>arap warningtime</b> <i>[minutes]</i>	Set the disconnect warning time.
9	<b>arap noguest</b>	Disallow guests.
10	<b>arap require-manual-password</b>	Require manual password entry.
11	<b>arap zonelist</b> <i>zone-access-list-number</i>	Limit the zones the Macintosh user sees.
12	<b>arap net-access-list</b> <i>net-access-list number</i>	Control access to networks.

## Monitor an ARA Server

To display information about a running ARA connection, perform the following task in privileged EXEC mode (reached by entering the **enable** command and a password):

Command	Purpose
<b>show arap</b> <i>[line-number]</i>	Display information about a running ARA connection.

The **show arap** command with no arguments displays a summary of ARA traffic since the router was last booted. The **show arap** command with a specified line number displays information about the connection on that line.

## Monitor the AppleTalk Network

The Cisco IOS software provides several commands that you can use to monitor an AppleTalk network. In addition, you can use Apple Computer's Inter•Poll, which is a tool to verify that a device is configured and operating properly. Use the commands described in this section to monitor an AppleTalk network using both Cisco IOS software commands and Inter•Poll.

To monitor the AppleTalk network, perform one or more of the following tasks:

Step	Command	Purpose
1	<b>show applealk arp</b>	List the entries in the AppleTalk ARP table.
2	<b>show appletalk interface</b> [brief] [type number]	Display AppleTalk-related interface settings.
3	<b>show appletalk macip-clients</b>	Display the status of all known MacIP clients.
4	<b>show appletalk macip-servers</b>	Display the status of MacIP servers.
5	<b>show appletalk macip-traffic</b>	Display statistics about MacIP traffic.
6	<b>show appletalk traffic</b>	Display the statistics about AppleTalk protocol traffic, including MacIP traffic.
7	<b>show appletalk zone</b> [zone-name]	Display the contents of the zone information table.

## Make ARA Connections

If you are a Macintosh user, you can use AppleTalk Remote Access (ARA) to connect to an AppleTalk network through a Cisco access server. The Cisco IOS Release 10.2 and later software supports ARA 2.0 and ARA 1.0 so that you can remotely dial in through asynchronous network devices using ARA to access AppleTalk services (such as file sharing and printing) elsewhere on the network. For example, you can dial in from an X.25 network and connect to an AppleTalk network through a router. To enable ARA and dial-in access, configure a virtual terminal (VTY) line on the router. You can also configure ARA on TTY lines.

Because there are no user commands for connecting to the network from your Macintosh client, the process is not described in this publication. To start a connection in most ARA client packages, you click the **Connect** button from within the client software.

## ARA Configuration Examples

This section contains the following examples of ARA configuration:

- Extended AppleTalk Network Configuration Example
- Extended Network in Discovery Mode Configuration Example
- ARA Configuration Example
- Connect to an AppleTalk Network over a Foreign Protocol Example
- Cable Range Expansion Example
- TACACS Username Authentication Configuration Examples
- Enable TACACS for ARA Authentication Examples

- Dedicated ARA Line Configuration Example
- Configure a Multiuse Line Example
- Configure Modified and Unmodified Scripts Example
- Configure an ARA Server Example
- Telebit T-3000 Modem Setup Example

### Extended AppleTalk Network Configuration Example

The following example configures the interface for an extended AppleTalk network. It defines the zones Orange and Brown. The cable range of one allows compatibility with nonextended AppleTalk networks.

```
appletalk routing
interface ethernet 0
  appletalk cable-range 1-1
  appletalk zone Orange
  appletalk zone Brown
```

### Extended Network in Discovery Mode Configuration Example

The following example configures an extended network in discovery mode. In Figure 102, access server A provides the zone and network number information to the interface when it starts.

#### Figure 102 Discovery Mode

Use the following commands to configure this extended network in discovery mode:

```
appletalk routing
interface ethernet 0
  appletalk cable-range 0-0 0.0
```

## ARA Configuration Example

The following example configures the router for ARA support, as described in the comments (lines beginning with an exclamation point [!]).

```

! Enable AppleTalk on the router
appletalk routing
!
interface Ethernet 0
 ip address 172.30.1.1 255.255.255.0
!
! On interface Ethernet 0, assign network number 103 to the physical cable and
! assign zone name "Marketing Lab" to the interface. Assign a zone name if
! you are creating a new AppleTalk internet. If the internet already exists,
! the zone and cable range must match exactly, or you can leave the cable
! range at 0 to enter discovery mode. The suggested AppleTalk
! address for the interface in this example is 103.1
interface Ethernet 0
 appletalk cable-range 103-103 103.1
 appletalk zone Marketing Lab
! Configure a username and password for the router.
username jake password sesame
! On lines 4 through 8, InOut modems are specified, the lines are configured
! to automatically start an EXEC session or enable AppleTalk, AppleTalk Remote
! Access Protocol is enabled, the modem speed is specified as 38400 bps, and
! hardware flow control is enabled.
line 4 8
 modem InOut
 autoselect
 arap enabled
 speed 38400
 flowcontrol hardware

```

---

**Note** You must set your terminal emulator to match the speed that you set for the line.

---

## Connect to an AppleTalk Network over a Foreign Protocol Example

The following example enables a Macintosh client running ARA on a remote network to connect across an X.25 network, through the router, to an AppleTalk network. In this example, VTY lines 0 through 19 are configured for ARA.

```

appletalk routing
line vty 0 19
 arap enable
 autocommand arap
 arap dedicated
 arap timelimit 45
 arap warningtime 5
 arap noquest
 arap require-manual-password
 arap net-access-list 611

```

The Macintosh client connects to any VTY line from 0 through 19. When the EXEC prompt appears, ARA begins automatically on the line (because of the **autocommand arap** command). The VTY lines 0 through 19 are dedicated to ARA dial-in clients, and those clients have a 45-minute time limit. Five minutes before the line is disconnected, a warning message appears, indicating that the session will be disconnected in five minutes. Guest access is denied, and manual password entry is required. The AppleTalk access list 611 has been applied to the VTY lines, meaning that access to other networks through these VTY lines has been limited.

### Cable Range Expansion Example

In the following example, the cable range is changed and the zone name is re-entered.

The initial configuration is as follows:

```
appletalk cable-range 100-103
appletalk zone Twilight Zone
```

The cable range is expanded as follows:

```
appletalk cable-range 100-109
```

At this point, you must re-enter the zone name as follows:

```
appletalk zone Twilight Zone
```

### TACACS Username Authentication Configuration Examples

In the following example for TACACS and Extended TACACS, line 1 is configured for ARA and username authentication is performed on a TACACS server:

```
line 1
login tacacs
arap enable
```

In the following example of AAA/TACACS+, line 1 is configured for ARA and username authentication is performed on a TACACS server:

```
line 1
login authentication
arap authentication
```

### Enable TACACS for ARA Authentication Examples

The following example shows regular TACACS enabled for ARA authentication:

```
line 3
arap use-tacacs
```

The following example shows AAA/TACACS+ enabled for ARA authentication:

```
line 3
aaa authentication arap
```

### Dedicated ARA Line Configuration Example

In the following example, line 2 is configured as a dedicated ARA line, user authentication information is configured on the ARA server, and guests are not allowed to make ARA sessions:

```
username jsmith password woof
line 2
arap dedicated
arap noguest
```

## Configure a Multiuse Line Example

In the following configuration, ARA is enabled on lines 2 through 16, username authentication is configured on the ARA server, and the lines are configured to automatically start an ARA session when an ARA user on a Macintosh attempts a connection:

```
username jsmith password woof
line 2 16
  autoselect
  arap enabled
  arap noquest
```

## Configure Modified and Unmodified Scripts Example

If you are currently using modified CCL scripts and want to migrate to nonmodified scripts, you can set your system to accept logins using both modified (CCL) and unmodified scripts by entering the following commands in line configuration mode:

```
autoselect arap
autoselect during-login
arap noquest if-needed
```

## Configure an ARA Server Example

The following example shows how to set up ARA functionality.

Log in to the router, use the **enable** command to enter your password if one is set, use the **configure** command to enter configuration mode, and add the following commands to your configuration:

```
appletalk routing
arap network 104 ARAP Dialin Zone
interface ethernet 0
  appletalk cable-range 0-0 0.0
  ! puts router in discovery mode
line 5 6
  modem inout
  speed 38400
  arap enabled
  autoselect
```

If you already know the cable-range and the zone names you need, include the information in the configuration file. If you do not know this information, perform the following steps to use the discovery mode to allow the Cisco IOS software learn about the AppleTalk network:

- Step 1** Permit the Cisco IOS software to monitor the line for a few minutes.
- Step 2** Log in and enter configuration mode.
- Step 3** Show the configuration again (using the **show startup-config** command).
- Step 4** Note the **appletalk cable-range** and **appletalk zone** variables.
- Step 5** Manually add the information in those two entries and add any user accounts.

```
appletalk cable-range 105-105 105.222
appletalk zone Marketing Lab
username arouser password arapasswd
! Add as many users as you need
```

- Step 6** Save the configuration.
- Step 7** Show the configuration again (using the **show startup-config** command) to make sure the configuration is correct.

### Telebit T-3000 Modem Setup Example

The following example describes how to set up a Telebit T-3000 modem that attaches to a router, which supports hardware flow control. The Macintosh will use a CCL script to configure the attached modem.

---

**Note** When you configure modems for ARA, turn off MNP4 error correction because it can cause connection failures for ARA 1.0 clients. For dedicated ARA lines, it is sufficient to turn off error correction completely in the modem; for multiuse lines it is preferable to leave all forms of non-MNP4 error correction enabled so that users of other protocols can achieve error-corrected connections. This restriction does not apply to installations that only receive calls from ARAP 2.0 clients.

---

Start with the modem at factory defaults. (The preferred configuration for hardware flow control is AT&F9.) Use the direct command if you have a terminal attached to the modem, or use the T/D Reset sequence described in the Telebit T-3000 manual to reset the modem to the &F9 defaults.

Attach a hardware flow control-capable cable between the modem and the device with which you are configuring the modem. (At this point, the modem is in hardware flow control mode, with autobaud-rate-recognition, and can detect your speed between 300 and 38,400 bps at 8-N-1. However, the modem must receive the flow control signals from the device to which you have the modem attached.)

Send the modem the following commands:

```
ATS51=6 E0 Q1 S0=2 &D3 &R3 S58=2 &W
```

This sequence directs the modem to perform the following tasks:

- Lock your DTE interface speed to 38,400 bps.
- Turn “command echo” off.
- Do not send any result codes.
- Auto-answer on the second ring (Germany requires this, but elsewhere you can set it to answer on the first ring with “s0=1”).
- When DTR is toggled, reset to the settings in NVRAM.
- CTS is always enabled if hardware flow control is disabled.
- Use full-duplex RTS/CTS flow control.
- Write these settings to NVRAM.

At this point, if you press the Return key or enter characters, no characters appear on your screen because the result codes are turned off. You can determine whether the modem is working by getting a list of its configuration registers using the following command:

```
AT&V
```

After the modem is configured, connect it to the router with a modem-to-RJ45 adapter and an RJ-45 cable to the lines(s) that you plan to use.

The following Cisco IOS commands are compatible with the Telebit 3000 settings described in this section:

```
line 1 8  
  arap enable
```

```
autoselect
no escape-character
flowcontrol hardware
modem dialin
speed 38400
```

